


KANSAS DEPARTMENT OF CORRECTIONS

	I NTERNAL M ANAGEMENT P OLICY AND P ROCEDURE	SECTION NUMBER 05-115	PAGE NUMBER
		SUBJECT: INFORMATION TECHNOLOGY AND RECORDS: Network Administration	

The IMPP has been placed on RESERVE status, reason being is that the viable content of this IMPP has been subsumed within the parameters of IMPP (05-171) being issued at this time.

Secretary of Corrections

06-02-04

Date

INTERNAL MANAGEMENT POLICY & PROCEDURES

STATEMENT OF ANNUAL REVIEW

IMPP # 05-115

Title: RECORDS: Network Administration

The above referenced Internal Management Policy and Procedure (IMPP), issued effective 11-21-01, was reviewed during January 2004 by the KDOC Policy Review Panel, per IMPP 01-101. At the time of this annual review, the Policy Review Panel determined that: no substantive changes and/or modifications to this IMPP are necessary at this time, and the IMPP shall remain in effect as issued on the above stated date.

The next scheduled review for this IMPP is January 2005.

This statement of annual review shall be placed in front of the referenced IMPP in all manuals.


Norman Bacon, IT Acting Director
Policy Review Committee Chairperson

Date

Roger Werholtz, Secretary of Corrections

02-03-04
Date

KANSAS DEPARTMENT OF CORRECTIONS

	INTERNAL MANAGEMENT POLICY AND PROCEDURE	SECTION NUMBER 05-115	PAGE NUMBER 1 of 4
		SUBJECT: INFORMATION TECHNOLOGY & RECORDS: Network Administration	
Approved By: Secretary of Corrections		Original Date Issued:	N/A
		Current Amendment Effective:	11-21-01
		Replaces Amendment Issued:	N/A

POLICY

The Division of Information Services and Communication (DISC) manages the Kansas State Network through the use of dedicated data circuits located throughout the state at all state agencies. The Kansas Department of Corrections is a subscriber to the data transmission service and does not have the right to alter or abuse them in any way.

The KDOC Information Resource Manager shall designate a Network Security Officer who shall be responsible for monitoring usage of the circuits as well as implementing appropriate security related to the KDOC network. Compliance with policy is the responsibility of all users in the department. Monitoring of circuits may be delegated to Network Administrators as approved by the NSO.

Any abuse and/or alteration of the network shall be reason for immediate termination of the specific circuit. Violations may result in disciplinary action in accordance with KDOC policies. Failure to observe Departmental policies and procedures affecting network operations may result in the proposal of disciplinary action by the appointing authority. The nature of the disciplinary action proposed shall depend upon the type and severity of the violation, whether it created any liability or loss to the Department, and whether or not a history of repeated violations existed at the time of the instant offence.

DEFINITIONS

D.I.S.C.: The Division of Information Services and Communication

Fire Wall: A software or hardware system which prevents or restricts the unauthorized access to or from a network.

Frame Relay Circuit: A special telephone line with available circuit speeds from 56 KB through a T1, used for data/voice/video transmissions.

Network: An internal or external series of devices physically and/or logically connected together to exchange information.

Network Security Officer: A person appointed/designated by the IRM who is responsible for the operation and security of a network.

Owner: Agency or other organizational entity that has responsibility for making communication judgments and decisions on behalf of the State with regards to identification, risk classification, value, and protection of the State's IT resources, or portion thereof.

Unauthorized Use/Access: Willfully, fraudulently and without authorization gaining or attempting to gain access to any computer, computer system, computer network or to any computer software, program, documentation, data or property contained in any computer, computer system or computer network.

User: Individual or organizational unit that is authorized to use IT resources.

Supplier of Service: Organizational unit that provides IT services to others or to itself in support of the State's mission and goals.

PROCEDURES

I. Responsibility of Establishing Connection to a Frame Relay Circuit

- A. The IRM shall be responsible for determining and/or approving the need and speed of a circuit based on the facility needs.
- B. The NSO shall be responsible for ordering circuits through DISC.
 - 1. The NSO shall prepare all necessary forms for submission to DISC, which contain all pertinent information regarding the connection.
 - 2. The NSO shall maintain logs detailing all information for the connection (i.e., circuit number, location, speed, number of users, etc).
 - 3. The NSO shall act as liaison between the facilities/offices and DISC or any other vendor in the connection to a network. Any deviance from this shall be approved by the NSO.
- C. Internal wiring or connection to the circuit shall be the responsibility of the requesting location unless approved by the NSO.
- D. Any deviation from standard network connections shall be submitted to the NSO for approval 60 days prior to the date the location requires connection/service:
 - 1. This shall include, but not be limited to:
 - a. Integrated Service Digital Network (ISDN);
 - b. Digital Subscriber Line (DSL);
 - c. Asymmetric Digital Subscriber Line (ADSL);
 - d. Wireless Local Area Network (WLAN)
 - e. Cable Modem, and/or
 - f. Desktop video.
 - 2. All requests for circuits and systems connected to the network must meet standards addressed in Kansas State Technical Architecture.

II. Network Security

- A. Any device connected to the KDOC network shall have, at a minimum, the following:
 - 1. Operating system with WIN NT/WIN 2000;
 - 2. Anti-virus system using standard department prescribed anti-virus software;

3. Standard hardware/software as prescribed in IMPP 05-111;
 4. Fire Wall, if location utilizes CJIS equipment.
 - a. The NSO shall be responsible for the management of all KDOC firewalls.
 - b. The NSO shall provide the IRM with monthly briefings of all rules applied to the firewalls during the month.
 - c. The NSO shall designate a regional team leader to serve as his back-up during any absences.
 - (1) All technicians shall be notified of the back-up designee.
 5. Internal/External modems shall not be operational while the device is connected to the network. Requests for exception will be temporary and must be approved by the NSO.
- B. The NSO shall prepare monthly reports regarding communication costs for budgetary controls.
- C. Logons and passwords shall not be disclosed to any person.
1. IT staff shall submit their ID and passwords to the NSO who shall maintain them in a secure location. These logons/passwords shall include, but not be limited to:
 - a. Servers;
 - b. Routers;
 - c. Switches;
 - d. Specialized network applications; and/or
 - e. Other devices and applications as required by the IRM.
- D. Any staff leaving KDOC service shall be immediately removed from any network access lists, including AS400 and e-mail.
- E. All devices shall be secure from sources of tampering, abuse and/or access from all non-authorized persons. These shall include, but not be limited to:
1. Personal Computers;
 2. Servers;
 3. Routers;
 4. Switches;
 5. Equipment Rooms;
 6. Wiring access areas; and/or
 7. Any location that would provide access to either the network or network devices.

III. Incident Reporting

- A. Any unauthorized use of a device or network connection shall be reported to the NSO. This shall include but not be limited to:
 - 1. Unauthorized use of a device by inmates,
 - 2. Surfing the Internet,
 - 3. Violations of password security protocols,
 - 4. Attempting to logon to a device not assigned to the user; and/or
 - 5. Loading applications not authorized by KDOC.
- B. All incidents shall be assigned a logging number by the NSO and forwarded to the appropriate facility information technology staff member for use in tracking all incidents.
- C. The IRM shall determine if the usage requires further investigation and/or submission to appropriate supervisory staff for possible proposal of disciplinary action.
- D. The NSO shall provide a monthly report of violations and network security issues to the IRM. This shall include, but not be limited to, those items in III.A above.

IV. Audits

- A. The NSO shall be responsible for conducting any/all necessary audits regarding the security of the KDOC network.
- B. Training shall be conducted utilizing current state audit material.

NOTE: The policy and procedures set forth herein are intended to establish directives and guidelines for staff and offenders and those entities who are contractually bound to adhere to them. They are not intended to establish State created liberty interests for employees or offenders, or an independent duty owed by the Department of Corrections to either employees, offenders, or third parties. This policy and procedure is not intended to establish or create new constitutional rights or to enlarge or expand upon existing constitutional rights or duties.

REPORTS REQUIRED

None.

REFERENCES

KSA 21-3755
DISC Standard Operating Procedures 1805.01 & 4206.01

ATTACHMENTS

None